

August 24, 2016

Via Electronic Filing

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street SW
Washington, DC 20554

Re: Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications (DSRC) Service in the 5.850-5.925 GHz Band (5.9 GHz Band), RM-11771

Dear Ms. Dortch:

On behalf of the Information Technology Industry Council (ITI), I write to urge the Commission to deny the above referenced petition. ITI's member companies are at the forefront of the convergence of technology and automobiles, and are committed to ensuring both consumers, and their privacy and security are protected as an increasing amount of technology is available in passenger and commercial vehicles.

As we elaborate below, however, we believe this petition should be rejected for three primary reasons: 1) significant work is being done elsewhere in the federal government with respect to automotive cybersecurity; 2) the FCC's expertise around cybersecurity and privacy reside in the areas in which it has clear authority and has traditionally regulated, which does not include automotive cybersecurity; and 3) the petition overstates the legal authority for the FCC to regulate automotive privacy and cybersecurity. Further, we believe DSRC is but one of many technologies under consideration for inclusion and, ultimately, deployment in connected automobiles.

Federal Work is Ongoing for Automotive Cybersecurity and Privacy

A number of federal agencies are engaged in ongoing work around automotive cybersecurity. In particular, the National Highway Traffic Safety Administration (NHTSA) has several ongoing efforts to address cybersecurity in automobiles. Directly related to DSRC for instance, NHTSA released documentation on July 21, 2016 for Vehicle-to-Vehicle (V2V) Public Key Infrastructure to in part address privacy and security of DSRC.¹

Furthermore, earlier this spring, NHTSA opened a request for comment on security for emerging technologies in automobiles to address new potential vulnerabilities as a result of increased

¹ See *Memorandum: Technical Design of the Security Credential Management System – Final Report*, Docket No. NHTSA-2015-0060, July 21, 2016.

technology and connectivity in vehicles.² Similarly, NHTSA has taken action within existing authority to address other V2V technology.³

Another step to address automotive security was taken in 2014 with the formation of the Automotive Information Sharing and Analysis Center (Auto ISAC).⁴ The Auto ISAC was formed in 2014, and in January of this year released a set of Proactive Safety Principles, with the fourth principle, “Enhance Automotive Security,” aimed at collectively addressing cybersecurity threats that could affect security. ISACs have been invaluable to other sectors, allowing industry to quickly respond to emerging threats. Other industry ISACs have been in existence for longer periods of time – for instance the Information Technology ISAC (IT-ISAC) was formed in 2000 and the Financial Services ISAC was launched in 1999 – and have developed best practices for effectively receiving, distilling and sharing threat information and working with the groups’ members. The ISACs play an invaluable role in helping to address sector specific, and cross-sectoral threats and vulnerabilities. For example, the IT-ISAC helped members monitor and collaborate with each other and other sectors on large-scale threats such as Conficker and the DNS Cache Poisoning Vulnerability. In those cases, the IT-ISAC provided a forum for members to engage in collaborative analysis on those significant issues, and to draft and share analytical alerts with remediation suggestions that were shared with members, partner ISACs, and the public. The Auto ISAC will similarly prove invaluable in helping the sector respond to real-time threats.

The automotive industry has also established “Consumer Privacy Protection Principles for Vehicle Technologies and Services” to protect personal information collected through in-car technologies. These Principles commit automakers to take certain steps to protect the personal data generated by their vehicles.⁵ The Principles establish a framework that automakers and other participants in the automotive industry may choose to adopt when offering innovative vehicle technologies and services. The Participating Members adopting this framework commit to seven Principles: Transparency; Choice; Respect for Context; Data Minimization, De-Identification & Retention; Data Security, Integrity & Access, and Accountability. The Principles’ fundamentals are based on the Federal Trade Commission’s (FTC) Fair Information Practice Principles (FIPPs), which, in turn, rest on privacy practice frameworks used in the United States and around the world for over forty years. Consistent with the FIPPs approach, the Principles treat sensitive information, such as geolocation, driver behavior, and biometric information, with additional, heightened protections.

² See Department of Transportation, Highway Traffic Safety Administration (NHTSA), Request for public comments Safety Related Defects and Emerging Automotive Technology, Docket ID NHTSA-2016-0040.

³ See NHTSA Advanced Notice of Proposed Rulemaking Vehicle-to-Vehicle Communications, Docket ID NHTSA 2014-0022-0002.

⁴ See www.autoisac.com for more information.

⁵ For more information and a list of automakers that have signed onto the Consumer Privacy Principles, see: www.AutomotivePrivacy.com.

Other Federal Agencies Have Greater Expertise in Automotive Cybersecurity and Privacy

In addition to NHTSA, others in the federal government are engaged in ongoing cybersecurity work that is applicable to the automotive sector. The tech sector as well as many other sectors voluntarily partnered with the National Institute of Standards and Technology (NIST) nearly three years ago for the development and promotion of the Framework for Improving Critical Infrastructure Cybersecurity (Framework).⁶ The Framework stems from Executive Order 13636,⁷ issued in February 2013, which called for the government to partner with owners and operators of critical infrastructure to improve cybersecurity through the development and implementation of risk-based standards. Framework development occurred through a process of coordination and collaboration convened by NIST between the technology industry, others in private industry, and USG partners. Taking a similar public-private partnership approach, NIST recently released a Draft Framework for Cyber-Physical Systems⁸ (CPS Framework) that was developed in partnership with industry, academic, and government experts. One of the key working groups in the cyber-physical systems project is focused on cybersecurity and privacy.⁹

ITI believes it is pivotal to continue to replicate the voluntary partnership approach embodied in the Framework in addressing cybersecurity challenges. The NIST Framework provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all critical infrastructure sectors, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats. The cyber-physical systems framework will provide additional technical details for building secure products for the IoT, including automobiles. We recommend that all regulators harmonize and streamline their approaches to addressing cybersecurity and privacy around the Framework approach.

The Petition Overstates the Case for FCC Authority to Regulate Edge Providers

At the outset, it is important to note that the petition itself recognizes that DSRC is not a common carrier service, and thus not subject to Section 222.¹⁰ Instead, the petition suggests, with little support or justification, that the FCC has supposed authority under Section 303(b) and 303(r), and also suggesting that a whole suite of new entities that utilize licensed spectrum for a wireless service should be subjected to FCC privacy and cybersecurity regulation. The petition makes this leap with an unsupported claim that “no one can doubt that the privacy and security of America’s drivers serves ‘the public interest, convenience and necessity.’”

The FCC’s stated authority for its proposed broadband privacy rules rely on Section 222, which

⁶ See Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), <http://www.nist.gov/cyberframework/index.cfm>.

⁷ See Executive Order 13636 Improving Critical Infrastructure Cyber Security, White House, <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

⁸ See CPS Draft Framework, NIST, <http://www.cpspwg.org>.

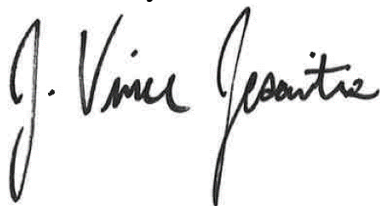
⁹ See CPS PWG Cybersecurity, NIST, http://www.nist.gov/cps/cpswpg_security.cfm.

¹⁰ See Petition, at viii.

provide for protections of consumer proprietary network information that telecommunications carriers collect from their customers. ITI filed comments in that proceeding that make clear that edge device and service providers are not subject those proposed rules.¹¹ There is a clear delineation between broadband internet access service providers and edge providers. The Commission specifically states in the privacy NPRM: “We recognize that edge providers, who may have access to some similar customer PI, are not subject to the same regulatory framework, and that this regulatory disparity could have competitive ripple effects. However, we believe this circumstance is mitigated by three important factors. First, the FTC actively enforces the prohibitions in its organic statute against unfair and deceptive practices against companies in the broadband ecosystem that are within its jurisdiction and that are engaged in practices that violate customers’ privacy expectations. We have no doubt that the FTC will continue its robust privacy enforcement practice. Second, the industry has developed guidelines recommending obtaining express consent before sharing some sensitive information, particularly geo-location information, with third parties, and large edge providers are increasingly adopting opt-in regimes for sharing of some types of sensitive information. Third, edge providers only have direct access to the information that customers choose to share with them by virtue of engaging their services; in contrast, broadband providers have direct access to potentially all customer information, including such information that is not directed at the broadband provider itself to enable use of the service.”¹² Acting favorably on this petition would clearly be in contrast to the points expressed by the Commission in the NPRM, ITI’s comments in that proceeding, and not recognize the significant work that is occurring around automotive cybersecurity and privacy across the federal government.

Given this, we urge the Commission to deny the above referenced petition and instead lend its support and relevant expertise in communications policy to other ongoing federal efforts to ensure our increasingly connected automobiles are safe, secure, and able to leverage the most cutting edge security technologies ITI’s member companies and the automotive sector are bringing to market.

Sincerely,



J. Vince Jesaitis
Vice President, Government Affairs

¹¹ See ITI comments in *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, May 27, 2016, at p 5-7.

¹² See *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at ¶ 132.